REMARKS

In the Office Action mailed on **13 June 2008**, the Examiner reviewed claims 1-4, 6-13, 15-22, and 24-30. Examiner rejected claims 1-4, 6-13, 15-22, and 24-30 under 35 U.S.C. § 103(a) based on Hermann (EPO Patent Publication No. EP1024626A1, hereinafter "Hermann"), and Stirbu (US Pub. No. 2003/0200431 hereinafter "Stirbu").

In the telephone interview conducted on **21 August 2008**, Applicant and Examiner discussed possible amendment options. Applicant proposed during the interview that the new amendment may include language to further clarify that the process of pre-authentication involves the steps of: (1) exchanging key commitment information between the provisioning device and the situation notification device over the preferred channel; (2) exchanging keys between the provisioning device and the situation notification device over a bidirectional communication channel which does not have to be the preferred channel; and (3) verifying the received keys using the received key commitment information on both the provisioning device and the situation notification device.

Examiner pointed out that the Applicant might consider further clarifying that the step of exchanging the key commitment information and the step of exchanging keys do not have to occur on the same channel (i.e., the preferred channel). Furthermore, Examiner suggested that the Applicant further clarify that the communication channels used to exchange the pre-authentication information are bi-directional channels, so as to distinguish the invention from Hermann. Examiner indicated during the interview that when these suggested changes are incorporated into the proposed amendment, the claims would be in condition for allowance.

Applicant agreed with the Examiner's suggestion changes and subsequently incorporated these changes into the amended claims.

Rejections under 35 U.S.C. §103

Independent claims 1, 10, and 19 were rejected under 35 U.S.C. § 103 based on Hermann and Stirbu. Examiner asserted that Hermann disclosed the process of pre-authenticating between user's personal device and the serving device in paragraphs [0021]-[0022] in Hermann.

Applicant respectfully points out that the pre-authentication used by the instant application involves the following steps: (1) exchanging key commitment information between the provisioning device and the situation notification device over the bidirectional preferred channel; (2) exchanging keys between the provisioning device and the situation notification device over a bidirectional channel which does not have to be the preferred channel; and (3) verifying the received keys using the received key commitment information on both the provisioning device and the situation notification device.

Note that the above pre-authentication process is different from the authenticating session disclosed by Hermann at least in the following aspects.

First, the pre-authentication process of the present invention involves separately exchanging authentication information by first exchanging key commitment information; and then exchanging keys. Note that these two exchanges are separate because they do not have to occur on the same communication channel (see paragraph [0069], lines 4-5 of the instant application). Also note that the above exchanges are bidirectional and hence are made over the respective **bidirectional communication channel(s).** In contrast, the authentication session of Hermann involves passing via **a unidirectional communication channel**, a sequence or an initial-sequence of authentication related information from the personal device to the serving device (see Hermann, paragraph [0021], line 5). Furthermore, Hermann did not disclose passing the key commitment information separately from passing the keys (see Hermann, [0021]).

In addition, the preferred channel where the exchange of key commitment occurs has a demonstrative identification property and an authenticity property, and does not require being resistant to eavesdropping. The demonstrative identification property allows a human operator to be aware of which devices are communicating with each other based on physical proximity. The authenticity property makes it difficult or impossible for attacking devices to tamper with or alter messages transmitted in the preferred channel, or to insert false information into the preferred channel without being detected by legitimate participants communicating via the preferred channel. See paragraphs p0051] – [0054] of the instant application. Neither Herman nor Stirbu discloses these features.

Secondly, the pre-authentication process of the present invention involves using the received key commitment information to verify the received keys **on both the provisioning device and the situation notification device without sending encrypted information back to each other** (see paragraph [0069] of the instant application). In contrast, Hermann performs authentication by sending back encrypted information from the serving device to the personal device. Note that this step also involves a number of differences. First, embodiments of the present invention perform authentication (i.e., verifying the keys) on each of the provisioning device and the situation notification device without having to return the encrypted information. This is possible because each device receives both key commitment information and keys, and hence can perform the key verification using the received information on the receiving device(s). Secondly, the present invention uses the key commitment information to verify the keys. In contrast, Hermann is mute on how the keys are authenticated.

Hence, there is nothing within Hermann and Stirbu, either separately or in concert, which suggests pre-authenticating the situation notification device involves: (1) exchanging key commitment information between the provisioning device and the situation notification device over the bidirectional preferred channel which as a demonstrative identification property and an authentication property; (2) exchanging keys between the provisioning device and the situation notification device over a bidirectional channel which does not have to be the preferred channel; and (3) verifying the received keys using the received key commitment information on both the provisioning device and the situation notification device.

Accordingly, Applicant has amended independent claims 1, 10, and 19 to clarify that the present invention provides a technique for pre-authenticating the situation notification device by: (1) **exchanging key commitment** information between the provisioning device and the situation notification device **over the bidirectional preferred channel** ; (2) **exchanging keys** between the provisioning device and the situation notification device **over a bidirectional channel which does not have to be the preferred channel**; and (3) verifying the received keys using the received key commitment information on both the provisioning device and the situation notification device. These amendments find support in paragraphs [0067]-[0071] of the instant application. No new matter has been added.

Additionally, Applicant has amended independent claims 1, 10, and 19 to further qualify the preferred channel as being "**bidirectional, location-limited, has a demonstrative identification property and an authenticity property**," and then specify that "**the demonstrative identification property allows a human operator to be aware of which devices are communicating with each other based on physical proximity; and the authenticity property allows legitimate devices communicating over the preferred channel to detect when an attacker transmits over the preferred channel or when an attacker tampers with messages sent over the preferred channel**." These amendments further differentiate the preferred channel used in the instant application from the communication channels described by Hermann and Stirbu, which did not include every feature listed within the above amendments. Note that these amendments find support in [0051]-[0053] of the instant application. No new matter has been added.

Hence, Applicant respectfully submits that independent claims 1, 10, and 19 are in condition for allowance. Applicant also submits that claims 2-4, 6-9, and 28, which depend upon claim 1, claims 11-13, 15-18, and 29, which depend upon claim 10, and claims 20-22, 24-27, and 30, which depend upon claim 19, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By __/Shun Yao/__________
Shun Yao
Registration No. 59,242

Date: 8 September 2008

Shun Yao
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1667
Fax: (530) 759-1665
Email: shun@parklegal.com